

Raspodijeljene glavne knjige i kriptovalute

Uvod i osnove kriptografije

Ante Đerek, Zvonko Konstanjčar



8. listopada 2021.

Nositelji

- Ante Đerek, ante.derek@fer.hr
- Zvonko Kostanjčar, zvonko.kostanjcar@fer.hr

Asistenti

- Stjepan Begušić
- Fredi Šarić
- Petar Paradžik
- Sven Goluža

- https://www.fer.unizg.hr/predmet/rgkk_b
- MS Teams grupa
- mailing lista rgkk@fer.hr
- Konzultacije po potrebi uz najavu mailom.

Nastava u akademskoj godini 2021./2022. odvijat će se kontaktno, uz propisane epidemiološke mjere, u skladu s uputama Ministarstva znanosti i obrazovanja.

- Preporuke za održavanje nastave na visokim učilištima u razdoblju pandemije bolesti COVID-19 uz primjenu protuepidemijskih mjera za akademsku godinu 2021./2022. (2. 9. 2021.).

Literatura (za prvi dio predavanja)

- A. Narayanan, J. Bonneau, E. Felten, A. Miller, S. Goldfeder (2016.), Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, dostupna na <http://bitcoinbook.cs.princeton.edu/>
- A. M. Antonopoulos (2015.), Mastering Bitcoin: Unlocking Digital Cryptocurrencies, dostupna na <https://github.com/bitcoinbook/bitcoinbook/blob/develop/book.asciidoc>

Slični predmeti

- Cryptocurrencies, blockchains, and smart contracts, <https://cs251.stanford.edu/>
- Bitcoin and Cryptocurrency Technologies, <https://www.coursera.org/learn/cryptocurrency>

Bodovanje

- Međuispit – 40%
- Završni ispit – 40%
- Prva laboratorijska vježba – 5%
- Druga laboratorijska vježba – 5%
- Seminar – 10%

Pragovi

- Zadovoljen minimum u obje laboratorijske vježbe.
- Ukupno 51% bodova iz svih komponenti.
 - Alternativno, ukupno 51% bodova iz pismenog ispita
- Pragovi za ocjene će biti objavljeni kasnije.

Prva laboratorijska vježba – Bitcoin transakcije i skripte

Okvirni datumi:

- Zadatak: 21.10.2021.
- Predaja vježbe: 1–5.11.2021.

Druga laboratorijska vježba – Ethereum pametni ugovori

Okvirni datumi:

- Zadatak: 02.12.2021.
- Predaja vježbe: 13–17.12.2021.

Osnovna pravila

- Možete raditi samostalno ili u grupi od najviše dvoje studenata. U slučaju grupnog rada oboje studenata mora biti upoznato sa svim aspektima svake vježbe.
- *Starter code* u programskom jeziku Java.
- Možete raditi u bilo kojem drugom programskom jeziku, ali bez podrške asistenata.
- U svakoj vježbi definiran minimum kojeg treba zadovoljiti za prag.

Važno!

- Strogo kažnjavanje pokušaja plagiranja (svih sudionika).
- Tražite pomoć od nastavnog osoblja dovoljno rano.

Osnovna pravila

- Možete raditi samostalno ili u grupi od najviše troje studenata.
- Nije obavezan!
- Možete izabrati neku od ponuđenih tema ili predložiti svoju.
- Teme će biti ponuđene nakon međuispita.

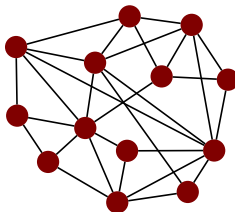
Accounts for Demo											
CASH ACCOUNT From 01.03.2003 to 29.02.2004 <input type="button" value="Select current year"/> <input type="button" value="Select previous year"/> <input type="button" value="Refresh list"/>											
Date	Payee	Reference	Category	Actual (gross)		Recon	Admin, fund split		Sink, fund split		Balance (net)
				Amount	Balance (gross)		GST net.	Non GST.	GST net.	Non GST.	
				0.00	0.00	<input checked="" type="checkbox"/>	0.00	0.00	0.00	0.00	0.00
25 MAY 01	Mr J Citizen	Lot 1 levy ps	Deposit	500.00	500.00	<input checked="" type="checkbox"/>	0.00	500.00	0.00	0.00	500.00
26 MAY 01	Local Insurance B	Insurance Ar	Insurance Bu	-269.00	231.00	<input checked="" type="checkbox"/>	0.00	-269.00	0.00	0.00	231.00
31 MAY 01	Netbank	Govt Debit Te	Govt Debit Te	-2.52	228.48	<input checked="" type="checkbox"/>	0.00	-2.52	0.00	0.00	228.48
31 MAY 01	Netbank	Account Ser	Account Ser	-5.00	223.48	<input checked="" type="checkbox"/>	0.00	-5.00	0.00	0.00	223.48
31 MAY 01	Netbank	Interest	Bank Interest	0.52	224.00	<input checked="" type="checkbox"/>	0.00	0.52	0.00	0.00	224.00
3 JUN 03	Clarkes Grounds	Grounds Mai	Grounds Mai	-30.00	194.00	<input checked="" type="checkbox"/>	0.00	-30.00	0.00	0.00	194.00
10 JUN 03	Electrical Enginee	Replace light	Building Main	-22.60	171.40	<input checked="" type="checkbox"/>	0.00	-22.60	0.00	0.00	171.40
11 JUL 03	Levy credit trans	Lot 1 credit tr	Levy credit tr	0.00	171.40	<input checked="" type="checkbox"/>	0.00	-250.00	0.00	250.00	171.40
10 OCT 01	Leahy	Terror Payou	Bank Transfe	1000.00	1171.40	<input type="checkbox"/>	909.09	0.00	0.00	0.00	1080.49
10 OCT 01	Fencers Upstand	Broken Pollin	Fencing	-120.00	1051.40	<input type="checkbox"/>	0.00	0.00	0.00	-120.00	960.49
16 OCT 01	Mr P D Jakson	Lot 1 levy ps	Deposit	400.00	1451.40	<input type="checkbox"/>	0.00	0.00	363.64	0.00	1324.13
6 NOV 03	Mr P D Jakson	Lot 1 levy ps	Deposit	25.00	1476.40	<input type="checkbox"/>	0.00	0.00	22.73	0.00	1346.86
11 NOV 01	Mr P D Jakson	Lot 1 levy ps	Deposit	5.00	1481.40	<input type="checkbox"/>	0.00	0.00	4.55	0.00	1351.41

Izvor: wikipedia.org

Što je raspodijeljena glavna knjiga?

Baza podataka koja je replicirana na mnoštvu čvorova u mreži.

- Svaki čvor održava svoju kopiju baze, podaci u svakom čvoru su identični.
- Postoji mehanizam koji omogućuje čvorovima da sinkroniziraju promjene i održavaju identične kopije.



Poželjna svojstva

Atomarnu promjenu baze obično nazivamo *transakcija*.

- *Integritet* – detalji transakcija se ne mogu izmijeniti.
- *Neizbrisivost* – transakcije se ne mogu izbrisati.
- *Autentičnost* – transakcije su ispravno autorizirane.
- *Neporecivost* – autorizacije transakcija se ne mogu poreći.
- *Ispravnost* – podaci su međusobno *konzistentni*.
- ...

Poželjna svojstva (nastavak)

- Sustav je *javan* – svatko može provjeriti ispravnost podataka, vršiti operacije na bazi, svatko može postati čvor u mreži.
- Sustav je *decentraliziran* – ne ovisi o nekom centralnom autoritetu.
- Sustav je *robustan* – funkcionira i kad je puno čvorova neispravno ili čak zlonamjerno.
- Postoji mehanizam *odgovornosti* – moguće je na neki način kazniti čvorove za neispravno ponašanje.
- ...

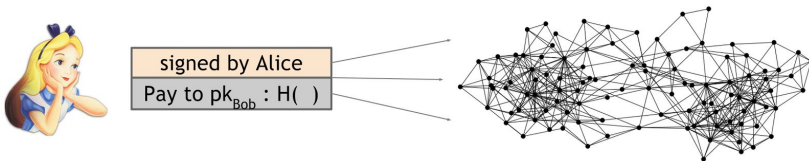
Pažnja!

Nemaju svi sustavi sva poželjna svojstva.

Ne znamo ostvariti *sva* poželjna svojstva *apsolutno*.

Kriptovaluta

Javna i decentralizirana raspodijeljena glavna knjiga u koju spremamo digitalno potpisane transakcije, a svaka transakcija opisuje promjenu vlasništva određene količine novca.



Izvor: bitcoinbook.cs.princeton.edu

Ishodi učenja

- 1 Definirati osnovne pojmove u tehnologiji raspodijeljene glavne knjige
- 2 Objasniti temeljnu tehnologiju transakcija, blokova, proof-of-work te izgradnju konsenzusa
- 3 Opisati razlike između najistaknutijih struktura ulančanih blokova
- 4 Analizirati platforme poput Ethereumu za izgradnju aplikacija temeljenih na ulančanim blokovima
- 5 Opravdati korisnost i vrijednost digitalnih valuta
- 6 Ocijeniti okruženja gdje se strukture temeljene na ulančanim blokovima mogu primijeniti, njihove potencijale i ograničenja
- 7 Prepoznati nove izazove u monetizaciji poslovanja vezanog uz kriptovalute i tehnologiju raspodijeljene glavne knjige

Razlike između kartičnog, gotovinskog (papirnatog) plaćanja i plaćanja kriptovalutom:

- Tko sve može plaćati i primiti novčana sredstva?
- Tko sve sudjeluje u transakciji?
- Kome su sve poznati podaci o transakciji?
- Koji nivo anonimnosti imaju sudionici?
- Je li potreban centralni autoritet?
- Može li se transakcija osporiti i opovrgnuti?

Odabrani dio povijesti

- 1988 – Chaum, Fiat, Naor, Untraceable electronic cash.
- 1989 – DigiCash.
- 1990's – Mondex, VisaCash.
- 1998 – HashCash (*proof-of-work* kao zaštita od spam-a).
- 2008 – Bitcoin whitepaper.
- 2009 – Prva Bitcoin transakcija.
- 2013 – Ukupna vrijednost svih Bitcoina prelazi 10^9 .
- 2014 – Blockchain 2.0 — Ethereum
- 2018 – RGKK na FER-u :)
- 2020 – The Beacon Chain, DeFi

Plan za sljedećih nekoliko predavanja:

- Kriptografska hash funkcija.
- Digitalni potpis.
- Jednostavne kriptovalute.
- Raspodijeljeni konsenzus.
- Bitcoin.

Osnovna svojstva

- Ulaz je niz bitova proizvoljne duljine.
- Izlaz je niz bitova fiksne duljine (npr. točno 256 bita).
- Funkcija je deterministička i može se brzo i efikasno izračunati.
- Funkcija je javna.

```
$ echo -n "fer" | sha1sum
cef48cb4569d34364e0e86067efa14fbe9b4591e  -
$ echo -n "fer" | sha1sum
cef48cb4569d34364e0e86067efa14fbe9b4591e  -
$ sha1sum big.txt
0c496df552232e34beaba1e15046f87e147d14f6  big.txt
$ sha1sum empty.txt
da39a3ee5e6b4b0d3255bfeef95601890afd80709  empty.txt
```

Izlazi kriptografske hash funkcije “izgledaju slučajno”...

```
$ echo -n "fer" | sha1sum
cef48cb4569d34364e0e86067efa14fbe9b4591e -
$ echo -n "fera" | sha1sum
e63c831418b7db691a469df5c15f405ecdade29a -
$ echo -n "Fer" | sha1sum
4514751a6511a102351de1f2b6abf0d6633c401f -
$ echo -n "fes" | sha1sum
a05b39a713e206dfa099e81182b9511af8b707f5 -
```

Hash funkcija H je ...

Otporna na kolizije

Ako je “praktički nemoguće” pronaći dvije različite poruke x i y takve da vrijedi $H(x) = H(y)$.

Korisna za slagalice

Ako je za svaki n -bitni *sažetak* y i za slučajno odabrani *prefix* k potrebno red veličine 2^n operacija kako bi se pronašao x takav da vrijedi $H(k||x) = y$ (dokle god k ima “dovoljno entropije”).

Kolizije uvijek postoje!

Ima beskonačno mogućih poruka, a 2^n mogućih sažetaka pa neke poruke moraju imati isti sažetak.

Za dobru kriptografsku hash funkciju vrijedi:

Jako je teško *pronaći* jednu jedinu koliziju, čak ako napadač ima na raspolaganju ogromne računalne resurse i puno vremena.


Napad grubom silom

- 1 Odaberi slučajnu poruku x .
- 2 Izračunaj $y \leftarrow H(x)$.
- 3 Zapamti par (y, x)
- 4 Ako je (y, x') već viđen za neki $x \neq x'$ onda smo našli koliziju.
- 5 Inače, idi na prvi korak.


Iz *paradoksa rođendana* slijedi da je potrebno red veličine $2^{n/2}$ koraka kako bi algoritam pronašao koliziju za hash funkciju čiji je sažetak veličine n bita.

SHAttered

The first concrete collision attack against SHA-1
<https://shattered.io>




Marc Stevens
Pierre Karpman




Elie Bursztein
Ange Albertini
Yarik Markov

SHAttered

The first concrete collision attack against SHA-1
<https://shattered.io>



Marc Stevens
Pierre Karpman



Elie Bursztein
Ange Albertini
Yarik Markov

```
└─ sha1sum *.pdf
38762cf7f55934b34d179ae6a4c80cadccb7f0a 1.pdf
38762cf7f55934b34d179ae6a4c80cadccb7f0a 2.pdf
└─ /tmp/sha1
└─ sha256sum *.pdf
2bb787a73e37352f92383abe7e2902936d1059ad9f1ba6daaa9c1e58ee6970d0 1.pdf
d4488775d29bdef7993367d541064dbdda50d383f89f0aa13a6ff2e0894ba5ff 2.pdf
```

0.64G 8-11h

Izvor: shattered.io

Zadatak: Pohrana u oblaku

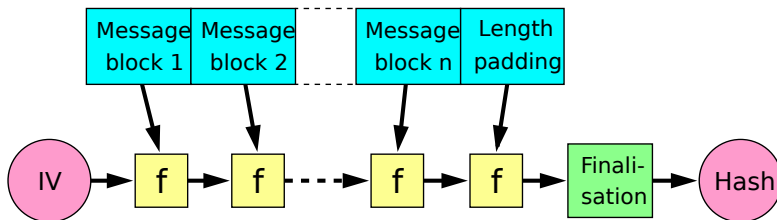
Spremate važnu datoteku na FER web kako bi je dohvatili s drugog računala. Kako možete biti sigurni da administratori nisu promijenili vašu datoteku?

Zadatak: Backup svih datoteka

Odredite koliko različitih datoteka postoji na disku vašeg računala i pronađite sve duplikate.

- Zaštita integriteta poruka.
- Zaštita zaporki.
- Generiranje pseudo-slučajnih brojeva.
- Digitalni potpis.
- ...

Merkle-Damgård konstrukcija (MD5, SHA1, SHA2, ...)



Izvor: wikipedia.org

Definicija

Hash pokazivač je pokazivač na neku poruku x zajedno s kriptografskim sažetkom te poruke $H(x)$. Dereferenciranje pokazivača uključuje ponovno računanje sažetka i uspoređivanje sa spremljenim.

```
path: /home/user/big.txt  
sha1: 0c496df552232e34beaba1e15046f87e147d14f6
```

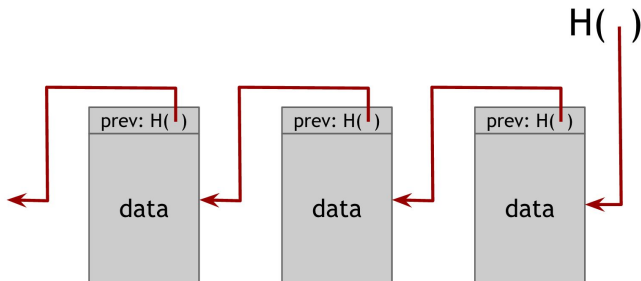
```
block_id: 4541244, transaction_id: 3426  
sha256: f6f0748717aca736bf18d5014279033f331a802348409ce305f908024fb2db46
```



Izvor: bitcoinbook.cs.princeton.edu

Definicija

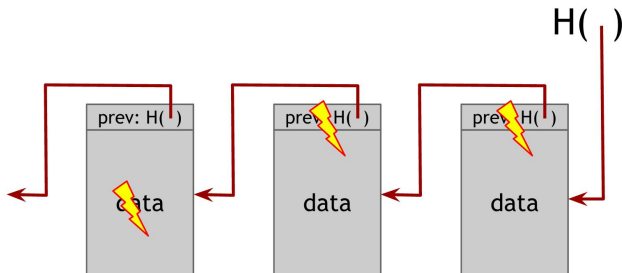
Kriptografski lanac blokova je jednostruko povezana lista u kojoj svaki element (uz neke podatke) sadrži hash pokazivač na prethodni element.



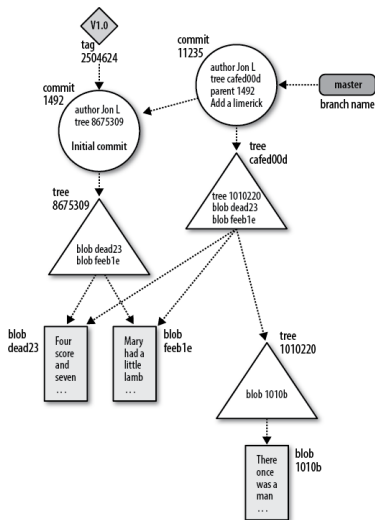
Izvor: bitcoinbook.cs.princeton.edu

Važno!

Hash pokazivač sadrži sažetak *cijelog* prethodnog bloka uključujući i njegov hash pokazivač.



Izvor: bitcoinbook.cs.princeton.edu



Izvor: Jon Loeliger, Matthew McCullough, Version Control with Git

```
https://www.fer.hr/lanac_diploma/master/2017.yaml
```

```
- previous_block:  
  block_id: 2016  
  block_uri: https://www.fer.hr/lanac_diploma/master/2016.yaml  
  block_hash: ade6629cd9b1fc5d55b88d7b09a82d621d9e513  
- block_id: 2017  
- student:  
  name: "Mirko Mirić"  
  oib: 123456789  
  graduation_date: "Sep 28 2017"  
- student:  
  name: "Slavko Slavić"  
  oib: 986198232  
  graduation_date: "Jul 01 2017"
```

Narodne novine, listopad 2017

FER čestita svim novim magistrima inženjerima!

Block: https://www.fer.hr/lanac_diploma/master/2017.yaml

Hash: a6d6be112ab1a22baebf38a6fe26674bb44e16b0

Zadatak

Kako poslodavac može provjeriti je li kandidat stvarno diplomirao na FER-u? Što ako je poslodavac stvarno paranoičan?

Zadatak

Ako www.fer.hr nije dostupan, kako student može dokazati da je stvarno diplomirao?

Zadatak

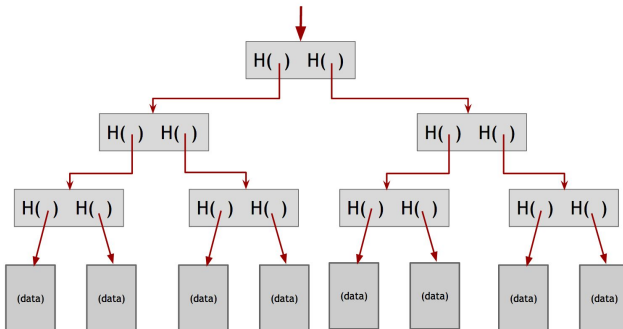
Što napadač mora napraviti kako bi dodao (ili uklonio) podatak da je neki student diplomirao 2010. godine?

*"The past was alterable. The past never had been altered.
Oceania was at war with Eastasia. Oceania had always
been at war with Eastasia."*

George Orwell, 1984

Definicija

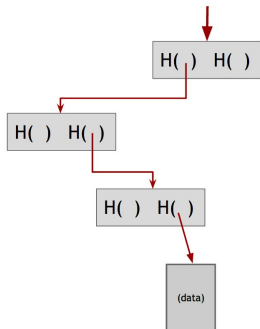
Merkleovo stablo je potpuno binarno stablo u kojem svaki unutarnji čvor sadrži hash pokazivače na svoja dva djeteta.



Izvor: `bitcoinbook.cs.princeton.edu`

Zadatak

Kako možemo nekoga uvjeriti da se određeni list stvarno nalazi u stablu?



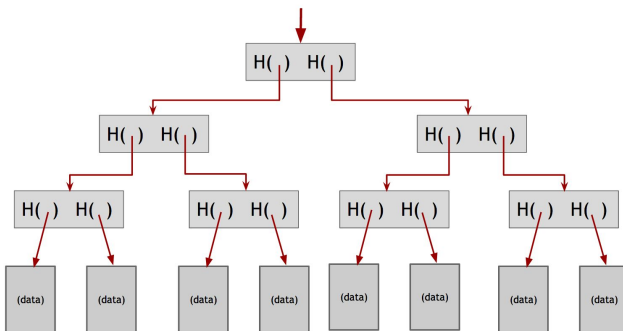
Izvor: bitcoinbook.cs.princeton.edu

Izazov

Kako možemo nekoga uvjeriti da element nije dio stabla?

Izazov

Kako možemo nekoga uvjeriti da element nije dio stabla?



Izvor: bitcoinbook.cs.princeton.edu